Important Information about «ISO/IEC 27001:2022» - Transition Period

Receiver: ISO/IEC 27001:2013 clients

Dear client,

The standard ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection — Information security management systems — Requirements" was released in October 2022 and is set to replace ISO/IEC 27001:2013.
The "International Accreditation Forum" (IAF) has issued a mandatory document IAF MD 26 containing transition requirements for new version of ISO/IEC 27001:2022 (2nd issue, dated 15.02.2023). All Information Security Management Systems (ISMS ISO/IEC 27001) Certification Bodies are required to implement the IAF MD document according to the defined dates.
The "International Accreditation Forum" (IAF) has defined a three-year transition period and some transitional arrangements. That means that after the transition period, any certification according to ISO/IEC 27001 must be based exclusively on the new edition, and all certificates based on the old edition become invalid, independent of the expiry date noted in the certificate.

Key Timescale
The following general conditions defined by IAF:

- Any initial certification audit and recertification audit starting on 01.05.2024 or later shall be performed based on ISO/IEC 27001:2022.

- All certifications based on ISO/IEC 27001:2013 will expire or be withdrawn at the end of the transition period (31.10.2025). Any certification decisions to convert existing ISO/IEC 27001:2013 certifications shall be completed by 31.10.2025 at the latest. Otherwise, a new full initial certification shall be performed.

Transition can be conducted in conjunction with the recertification or surveillance audits or through a separate "special case" audit.

Key changes

Compared with ISO/IEC 27001:2013, the main changes of ISO/IEC 27001:2022 include, but are not limited to:

1) Annex A references the information security controls in ISO/IEC 27002:2022, which includes the information of control title and control.

2) The notes of Clause 6.1.3 c) are revised editorially, including deleting the control objectives and using "information security control" to replace "control".

3) The wording of Clause 6.1.3 d) is re-organized to remove potential ambiguity.

4) Adding a new item 4.2 c) to determine the requirements of the interested parties addressed through an information security management system (ISMS).

5) Adding a new subclause 6.3 - Planning for changes, which defines that the changes to the ISMS shall be carried out by the organization in a planned manner.

Important Information about «ISO/IEC 27001:2022» - Transition Period

Receiver: ISO/IEC 27001:2013 clients

6) Keeping the consistency in the verb used in connection with documented information, for example, using "Documented information shall be available as evidence of XXX" in clauses 9.1, 9.2.2, 9.3.3 and 10.2.

7) Using "externally provided process, products or services" to replace "outsourced processes" in Clause 8.1 and deleting the term "outsource".

8) Naming and reordering the subclauses in Clause 9.2 - Internal audit and 9.3 - Management review.

9) Exchanging the order of the two subclauses in Clause 10 - Improvement.

10) Updating the edition of the related documents listed in Bibliography, such as ISO/IEC 27002 and ISO 31000.

11) Some deviations in ISO/IEC 27001:2013 to the high-level structure, identical core text, common terms and core definitions of MSS are revised for consistency with the harmonized structure for MSS, for example, Clause 6.2 d).

What the client shall do

For each organization, the extent of change required depends on the maturity and effectiveness of the current information security management system (ISMS), organizational structures and processes/procedures.

Organizations that have implemented ISMS, in order to identify the impact of the changes in ISO/IEC 27001:2022, are strongly recommended to take the following actions:

- Conduct a gap analysis identifying gaps that need to be addressed in order to meet new requirements.
- Preparation of a transition plan.
- Update the existing ISMS.
- Implementation and effectiveness of new information security controls and modifications introduced by organization.
- Provide appropriate training and build awareness for all parties that influence the effectiveness of the ISMS.
- Conduct an internal audit (an evaluation of the management system according to the new edition of ISO/IEC 27001:2022) and a management review prior to the transition audit being conducted.

For further information on this document, contact us. We look forward to continuing our good cooperation.